Some Thoughts about Applying STAMP to Environmental-Sociotechnical Systems (ESTS) – Very Complex System of Systems (SoS)

Second STAMP Conference
2013

Daniel Hartmann, PhD
Management & Safety Engineering Unit, Ben-Gurion University
Beer Sheva, Israel
A wider look at STAMP (System-Theoretic Accident Model and Processes)

- System Theory
- Hierarchical Safety Control Structure
- Process Models
- Safety Constraints
Data is the lowest level of abstraction, collected by "sensors" and leading to describing “something” or a process.

Information is a medium level of abstraction, processed by "brain" and an exciting "model" and leading to understanding of "something" or a process.

Knowledge is the highest level of abstraction, processed by "brain" and an exciting "model" and leading to action related to "something" or a process.
However, Risk is dictated by D.I.K.C.

- **Virtual Risk**
  - Perceived directly: e.g. using fire, cutting with a knife, climbing a tree
  - Perceived through science: e.g. cholera need a microscope to see it and a scientific training to understand it

**Natural DIKC**
- System 1 thinking

**Scientists don't know yet or cannot agree:** e.g. global warming, mobile phones

**Virtual DIKC**

**Scientific DIKC**
- Complexity
- System 2 thinking

*After Adams (1999)*
More Fundamentals dictating level of acceptable Risk

Technological Feasibility

Scientific Risk

Virtual Risk

Natural Risk

Economical Feasibility

Cultural Feasibility
One Picture - Two Perceptions

Perception is the process of attaining awareness or understanding of the situation by organizing and interpreting sensory information.

Who's Perception? Who Creates it? Who Controls it? Etc...

- "End User"?
- "Scientists"?
- Low Level Controller?
- Medium Level Controller?
- High Level Sociotechnical Controller?
- High Level Environmental Controller?
A wider look at STAMP
(System-Theoretic Accident Model and Processes)

- Data – Information – Knowledge – Context
  [D.I.K.C.]
- System Theory
- Hierarchical Safety Control Structure
- Process Models
- Safety Constraints
Environmental System of Systems

The Water Cycle

- Volcanic steam
- Ice and snow
- Precipitation
- Snowmelt runoff
- Infiltration
- Seepage
- Streamflow
- Freshwater
- Plant uptake
- Groundwater discharge
- Groundwater storage
- Water in the atmosphere
- Sublimation
- Desublimation
- Evapotranspiration
- Evaporation
- Condensation
- Fog drip
- Surface runoff
- Dew
- Oceans
- Vents and volcanoes

U.S. Dept. of the Interior
U.S. Geological Survey
John Evans, Howard Perlman, USGS
http://淡水.usgs.gov/divewatercycle.html
Environmental System of Systems
The Rock Cycle

[Diagram of the rock cycle showing the processes of sedimentation, metamorphism, and igneous activity.]
Environmental System of Systems

Eco-Systems
Modern Battlefield and the Environment
Some “New” Ideas about System Boundaries

Egocentric → System-centric
Sociotechnical → Environmental-Sociotechnical
Effort vs. Importance*

Currently

Effort Expended

Importance

- Latent System Weaknesses
- Human Failure
- Equipment Failure

Actual

A wider look at STAMP
(System-Theoretic Accident Model and Processes)

- System Theory
- Hierarchical Safety Control Structure
- Process Models
- Safety Constraints
Example Safety Control Structure

Where starts System safety Engineering?
Environmental-Sociotechnical System
Force Majeure - Superior Force - Act of God - Chance Occurrence - Unavoidable Accident

Resulting from:
- hurricane
- flooding
- earthquake
- volcanic eruption
- Virus pandemic
- Fire
- Dust storm
- Any unexpected / extreme environmental conditions
- etc.
Accident Causality Using STAMP

Enough D.I.K.C. at each system level?

Develop D.I.K.C. Metrics!
## Generic model for safety management system

<table>
<thead>
<tr>
<th>Level N+1 Goals, Policies, Constraints, Control Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference Channel</td>
</tr>
<tr>
<td>Measuring Channel (Feedback)</td>
</tr>
<tr>
<td>Level N Operational Experience</td>
</tr>
</tbody>
</table>

### Policy
- Conflicting Policies
- Biased Policies
- Partial correct Policies
- Wrong Policies
- Unrealistic Policies
- Disastrous Policies
- Etc.

### Diagram:
- Management Review
- Planning
- Checking & Corrections
- Implementation

---

Daniel Hartmann  STAMP 2013
System Dynamics perspective on Forest Fire

[Diagram showing interactions between fire prevention, fuel availability, fire intensity, and policy goals.]
Mount Carmel [Israel] forest fire (2010)
a very expensive lesson in risk management and safety
Reckoning without one’s host
(die Rechnung ohne den Wirt machen)

- To act, plan, or conclude without adequate consideration of significant factors or circumstances;
- to fail to take into account the role of others, particularly those whose position would make their input determinative.
- This early meaning, dating from the 17th century, has been totally lost in the now figurative one indicating shortsightedness, improvidence, or lack of foresight.
A wider look at STAMP
(System-Theoretic Accident Model and Processes)

- Data – Information – Knowledge – Context
  [D.I.K.C.]
- System Theory
- Hierarchical Safety Control Structure
- Process Models
- Safety Constraints
Accidents occur when model of process is inconsistent with real state of process and controller provides inadequate control actions.

**Process Models**

1. Goal Condition
2. Model Condition
3. Action Condition
4. Observability Condition

Feedback channels are critical

-- Design
-- Operation

**enough D.I.K.C. to create Models?**

1. Controller
2. Model of Process
3. Control Actions
4. Feedback

Controlled Process
A Classification of Control Flaws leading to Hazards

1. Inadequate Control Algorithm
   (Flaws in creation, process changes, incorrect modification or adaptation)

2. Missing or wrong communication with another controller

Controller

Control input or external information wrong or missing

Inadequate or missing feedback

Sensor

Feedback Delays

Inadequate operation

Incorrect or no information provided

Measurement inaccuracies

Controller

Controller

Inadequate operation

Sensor

Feedback Delays

Controller

Inappropriate, ineffective, or missing control action

Actuator

Inadequate operation

Controller

Delayed operation

Controller

Conflicting control actions

Process input missing or wrong

Controlled Process

Component failures

Changes over time

Unidentified or out-of-range disturbance

Process output contributes to system hazard

Component failures

Changes over time

D.I.K.C. Flaws leading to Hazards

Daniel Hartmann

STAMP 2013
A wider look at STAMP
(System-Theoretic Accident Model and Processes)

- System Theory
- Hierarchical Safety Control Structure
- Process Models
- Safety Constraints
Safety Constraints
Should be based on D.I.K.C.: Data, Information, Knowledge & Context

- Based on D.I.K.C. Each component in the control structure has
  - Assigned responsibilities, authority, accountability
  - Controls that can be used to enforce safety constraints

- Based on D.I.K.C. Each component’s behavior is influenced by
  - Context (milieu) in which operating
  - Level of Data, Information, Knowledge about current state of process

Accidents occur when models (because of D.I.K.C.) do not match process and:

- Required control commands are not given
- Incorrect (unsafe) ones are given
- Correct commands given at wrong time (too early, too late)
- Control stops too soon

Explains software errors, human errors, component interaction accidents, and errors due to level of DIK ...
Human Sensitivity to Environmental Hazards

[Graph showing damage thresholds and extremes over time]

- Upper extreme
- Lower extreme

Physical element

Time

Average

Band of tolerance

Hazard

Resources

Hazard

A
B
C

Cosmological Climate?

Geological Climate

Contemporary Climate

Weather

Climate Change

Hazardous System State

Inadequate Enforcement of Safety Constraints on Process Behavior

Process
Another Source of Risk

- Control actions inadequately “coordinated” among multiple controllers

Boundary areas: Environmental conditions are “normal”

Overlap areas: Environmental conditions are “extreme”
Safety as a dynamic Control Problem

Sociotechnical system:

“enforce safety constraints on Sociotechnical system behavior”

Environmental-Sociotechnical system:

“enforce safety constraints on Sociotechnical system behavior and avoid confrontation with Environmental system behavior”

Dutch: Living / Building with Nature